CHAPTER 4

Cisco Unified MeetingPlace システムの安全性およびセキュリティの確立

他の企業全体リソース（ネットワーク、電子メール、音声メールなど）の場合と同様に、Cisco Unified MeetingPlace のインストールおよび設定でもセキュリティは重要な問題になります。外部のユーザや以前の従業員のほか、現在の従業員によってもシステムが危険にさらされる可能性があります。システムのセキュリティについて計画するときは、全体的な利用しやすさも考慮してください。

この章は、次の項で構成されています。

安全上の注意事項および要件

セキュリティの面で考慮する事項としては、次のものがあります。

- 正規の会議への権限のないユーザの参加
- 必要な権限を持っていない会議のスケジュール、およびその会議への参加
- アウトダイヤルの濫用および不正通話
- システム管理者プロファイルを使用した、システム設定およびシステム パラメータへの不正アクセス

Cisco Unified MeetingPlace システムのセキュリティ パラメータ設定に加えて、いくつかのベスト プラクティス（「セキュリティのベスト プラクティス」を参照）を組織で実践すると、セキュリティを大幅に強化できます。認定インストレーション パートナー、または Cisco Advanced Services の担当者は、Cisco Unified MeetingPlace のセキュリティについてシステム管理者に説明し、システムの設定とベスト プラクティスの作成を支援して、セキュリティ保護された会議環境を確立できるようにします。

セキュリティのベスト プラクティス

システムのセキュリティを確立して維持するときは、次のガイドラインに従ってください。

- P.4-3 の「ワークシート 4-1：セキュリティ パラメータ」の表にあるセキュリティ パラメータの設定を含めて、ユーザ プロファイルおよびグループ プロファイルに関するポリシーを策定し、導入します。
- システム管理者権限を持つユーザ プロファイルの数は、できる限り少なくします。これらのアカウントの ID およびパスワードは長めにして、頻繁に変更するようにします。
- 可能な場合には、Cisco Unified MeetingPlace Directory Services をインストールする、または組織の人事データベースに対して追加と削除を実行するスクリプトを手動で作成することにより、ユーザ プロファイルに関するこれらの操作のプロセスを自動化します。いずれの方法を採用する場合でも、退職した従業員のプロファイルは必ず削除するか、無効にします。この両方のオプションについての詳細情報は、Cisco Unified MeetingPlace サポート組織が提供できます。
- プロファイルの処理を自動化できない場合は、組織の人事グループからの情報に基づいて、日常的に頻繁に行う追加と削除について手順書を作成し、順守します。特に重要になるのは、退職した従業員のユーザ プロファイルをただちに無効化または削除することです。
- 推測しにくく、かつユーザが覚えやすいプロファイル番号の作成規則を決定します。たとえば、電話内線は一般に推測されやすいため、プレフィクスを付加します。ランダム攻撃にさらされる危険がない場合は、従業員 ID も使用できます。セキュリティ上の理由から、プロファイル番号には少なくとも 7 桁が含まれるものを選択することをお勧めします。
- デフォルトのプロファイル パスワードが推測されにくいものであることを確認し、ユーザにただちに変更させます。レポートを定期的に実行して、デフォルトから変更されていないプロファイル パスワードを特定し、ユーザへの連絡、パスワードの変更、またはプロファイルの無効化あるいは削除を行って対処します。
- プロファイル パスワードに関するポリシーを策定して通知し、ユーザがありふれたパスワードを選択しないようにします。たとえば、同じ数字パターンの繰り返しや同じ数字の連続を含んだパスワードの作成を禁止します。
- エンド ユーザ コミュニティに対して、会議をセキュリティで保護する方法に関するヒント集を提供します。会議をセキュリティで保護する手段としては、一意の会議 ID、単純でない会議 ID、入席のアナウンス、会議のパスワード、参加の制限、会議のロック、望ましくない参加者の削除、およびロール コールがあります。
- 望ましくないアクセスがないかどうかについて、日常的にシステムを監視するポリシーを策定し、導入します。このような監視の主要な手段となるのは、レポートとアラームです。
- さまざまなタイプの不正アクセスへの対処について、計画を作成します。特に、Cisco Unified MeetingPlace Audio Server のセキュリティ パラメータの変更、その他のシステム アクセスに対する変更（電話番号の変更など）、および組織内での手順の変更について取り決めます。
- Cisco Unified MeetingPlace Audio Server は、ファイアウォールの内側にあるネットワーク内の保護区域に配置します。このシステムは、外部から直接アクセスする必要は一切ありません。
- MeetingTime が使用する TCP ポート（ポート 5001）が、ファイアウォールでブロックされていることを確認します。インターネット経由での MeetingTime の使用を許可することは、お勧めしません。
- Cisco Unified MeetingPlace 8106 または 8112 に SSH をインストールし、Telnet の使用を無効にすることを検討します。輸出規制に適合するために、SSH はベース ソフトウェア リリースとは別にインストールされることに注意してください。
- Cisco Unified MeetingPlace Audio Server に対する SNMP クエリーを無効にすることを検討します。クエリーを無効にしても、アラーム条件を示す SNMP トラップは引き続き生成されることに注意してください。
- technician のコマンドライン パスワードが、工場出荷時のデフォルト（ユーザ名が *admin*、パスワードが *cisco*）から変更されていることを確認してください。
- さまざまな統合アプリケーション製品、特にネットワークの保護区域外に配置される製品については、アップグレードして GWSIM 5.0 以降を使用することを検討してください。GWSIM 5.0 では、Cisco Unified MeetingPlace Audio Server との通信に暗号化データ ストリームが使用されます。また、サーバで生成されるデータ ストリームを使用してサーバと通信することもできるため、ファイアウォールで必要となるホールの数が少数で済みます。

ワークシート 4-1：セキュリティ パラメータ

次のワークシートは、システムをセキュリティ保護するときに利用できるセキュリティ パラメータを示しています。

「電話機経由で」と言及していない場合、および特定のタブについて言及していない場合は、どのパラメータも MeetingTime の Configure タブにあります。

パラメータ	説明	場所	オプション	デフォルト
システム アクセス				
Min profile pwd length	プロファイル パスワードの最小長	使用状況パラメータ	0 ～ 11	6
Change profile pwd (days)	プロファイル パスワードの変更が必要となる頻度	使用状況パラメータ	0 ～ 3650	90
Min user pwd length	ユーザ パスワードの最小長	使用状況パラメータ	0 ～ 11	5
Change user pwd	ユーザ パスワードの変更が必要となる頻度	使用状況パラメータ	0 ～ 3650	90
Max profile login attempts	プロファイルがロックされるまでに許可されるログイン試行回数	使用状況パラメータ	0 ～ 32767	3
会議のスケジュールと設定				
Allow vanity mtg IDs?	ユーザがスケジュールする会議に対して、ユーザによるカスタマー会議 ID の割り当てを許可するかどうか	System Parameters	Yes/No	Yes
Minimum mtg ID length	会議 ID の最小長	スケジューリング パラメータ	1 ～ 9	4
Min meeting pwd length	会議パスワードの最小長	使用状況パラメータ	0 ～ 11	0
Password required?	スケジュール時に、ユーザにパスワードの設定を要求するかどうか	User Profiles および User Groups	Yes/No	No
Display mtg to everyone?	このユーザがスケジュールした会議を表示できるメンバーを限定するかどうか (*Yes* を指定すると、このユーザがスケジュールした会議は誰でも Cisco Unified MeetingPlace Web Conferencing の会議を選択するリンクまたは MeetingTime の待合室で表示できます。値は、ユーザが会議をスケジュールするときに会議ごとに変更できます。)	User Profiles および User Groups	Yes/No	No
Allow guest outdial?	ゲストにアウトダイヤル権限を付与するかどうか (*Yes* にした場合は、ゲスト ユーザが Web から会議への参加ボタンをクリックしたときに、システムからゲスト ユーザにアウトダイヤルできます。会議のスケジュール担当者が会議ごとに値を変更できるのは、プロファイルの Can Schedule Guest Outdial Mtgs パラメータが *Yes* の場合のみです。)	User Profiles および User Groups	Yes/No	No

パラメータ	説明	場所	オプション	デフォルト
Scheduling restrictions	ユーザが会議をスケジュールできるかどうか (ユーザが 6 時間でスケジュールできる会議の数は、Near Term Mtg Limit の値によって決まります)	User Profiles および User Groups	Unrestricted、Cannot Schedule、または Near Term Mtg Limit	Unrestricted
会議アクセス				
Can schedule guest outdial mtgs?	ゲストが Web 経由で音声会議に参加できる会議を、ユーザがスケジュールできるかどうか (*Yes* を指定すると、Allow Guest Outdial in Mtgs パラメータをユーザが会議ごとに変更できるようになります)	User Profiles および User Groups	Yes/No	Yes
Entry announcement	会議参加者が会議に入席したときに、アナウンスするかどうか (*Beep+Name* を指定すると、すべてのゲストが会議入席前に名前の記録を求められます。名前を明示しないまま入席したゲストは、他の参加者によって明示を求められます。)	User Profiles および User Groups	Beep only/ Beep+Name、または None	Beep+Name
Allow Internet access?	Cisco Unified MeetingPlace システムの構成で、Web Conferencing サーバの 1 つが DMZ にあり、別の Web 会議サーバが DMZ の背後にあるとします。*Yes* にすると、会議の Web コンポーネントは DMZ にあるサーバで保持され、誰でもアクセスできるようになります。*No* にすると、会議の Web コンポーネントは DMZ の背後のサーバで保持され、企業のイントラネット上のユーザのみがアクセスできるようになります。	User Profiles および User Groups	Yes/No	No